(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
27 février 2003 (27.02.2003)

PCT

(10) Numéro de publication internationale
WO 03/017210 A1

(51) Classification internationale des brevets[7] : G07C 9/00, G06F 1/00

(21) Numéro de la demande internationale :
PCT/FR02/02874

(22) Date de dépôt international : 13 août 2002 (13.08.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/10832 14 août 2001 (14.08.2001) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **ATMEL NANTES SA** [FR/FR]; La Chantrerie, BP 70602, F-44306 Nantes Cedex 2 (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **DEBELLEX, Olivier** [FR/FR]; 21, avenue du Ponant, F-44300 Nantes (FR).

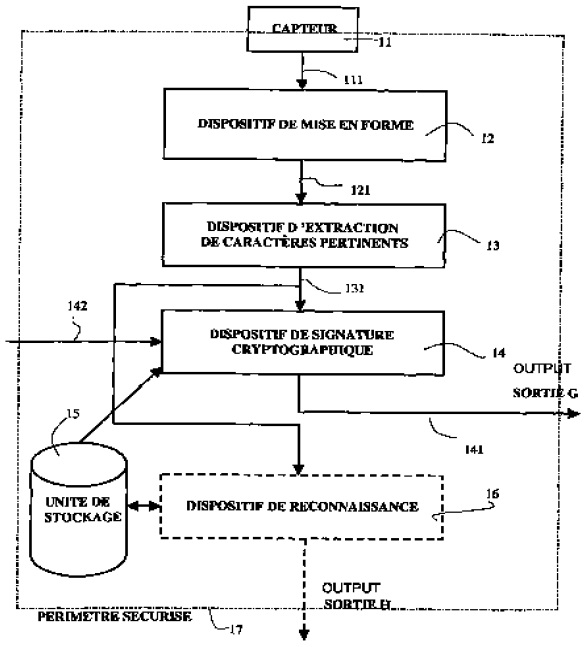
(74) Mandataire : **VIDON, Patrice**; Le Nobel, 2, allée Antoine Becquerel, BP 90333, F-35703 Rennes Cedex 7 (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM,

[Suite sur la page suivante]

(54) Title: DEVICE AND METHOD OF RECOGNISING AT LEAST ONE INDIVIDUAL, THE CORRESPONDING ACCESS CONTROL DEVICE AND SYSTEM AND APPLICATIONS THEREOF

(54) Titre : DISPOSITIF ET PROCEDE DE RECONNAISSANCE D'AU MOINS UN INDIVIDU, DISPOSITIF ET SYSTEME DE CONTROLE D'ACCES ET APPLICATIONS CORRESPONDANTES



11 SENSOR
12 FORMATTING DEVICE
13 DEVICE FOR EXTRACTING PERTINENT CHARACTERS
14 CRYPTOGRAPHIC SIGNATURE DEVICE
15 STORAGE UNIT
16 RECOGNITION DEVICE
17 SECURE PERIMETER

(57) Abstract: The invention relates to a device and method for the recognition of at least one individual and to the corresponding access control device and system and application thereof. The inventive recognition device comprises a one-piece integrated circuit which is produced by integrating the following elements on a silicon substrate: at least one biometric information sensor; means of processing said biometric information; cryptographic means which deliver at least one piece of encrypted data that is representative of at least one part of said biometric information and/or a corresponding piece of recognition information; and protection means that block access to data in transit, stored and/or processed in said one-piece integrated circuit in order to create a secure perimeter. In this way, the data exchanged by said sensor(s), processing means and cryptographic means, and particularly the aforementioned biometric information, are only saved in the one-piece integrated circuit and cannot be accessed from outside. Moreover, only encrypted data are delivered to the outside from said one-piece integrated circuit.

(57) Abrégé : Dispositif et procédé de reconnaissance d'au moins un individu, dispositif et système de contrôle d'accès et application correspondants. L'invention concerne un dispositif de reconnaissance d'au moins un individu, comprenant, dans un circuit intégré monolithique obtenu par l'intégration sur un même substrat de silicium de: au moins un capteur d'informations biométriques, des moyens de traitement desdites informations biométriques, des moyens cryptographiques, délivrant au moins une donnée cryptée représentative d'au moins une partie desdites informations biométriques et/ou d'une

[Suite sur la page suivante]

WO 03/017210 A1

HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* **:** brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

information de reconnaissance correspondante, et des moyens de protection, empêchant l'accès aux données transitant, stockées et/ou traitées dans ledit circuit intégré monolithique, pour former un périmètre sécurisé, de façon que les données échangées par le ou lesdits capteurs, lesdits moyens de traitement et lesdits moyens cryptographiques, et notamment lesdites informations biométriques, soient conservées uniquement dans ledit circuit intégré monolithique, restant inaccessibles depuis l'extérieur, et que seules des données cryptées soient délivrées à l'extérieur dudit circuit intégré monolithique.

DISPOSITIF ET PROCEDE DE RECONNAISSANCE D'AU MOINS UN INDIVIDU, DISPOSITIF ET SYSTEME DE CONTROLE D'ACCES ET APPLICATIONS CORRESPONDANTES

Le domaine de l'invention est celui de la biométrie, c'est-à-dire de la reconnaissance ou de l'identification d'individus à partir de certaines de leurs caractéristiques biométriques (empreinte digitale, empreinte vocale, empreinte oculaire, ...), notamment dans le cadre d'applications prévoyant un accès sécurisé à des lieux, des objets et/ou des données.

Plus précisément, l'invention concerne la sécurisation de la mise en œuvre de capteurs biométriques.

L'utilisation de la reconnaissance de caractéristiques biométriques pour le contrôle d'accès est une technique bien connue en soi, tant pour accéder à un site ou à une pièce protégée qu'à des données stockées dans une base de données. Les systèmes de ce type comprennent un capteur, par exemple pour relever une image d'une empreinte digitale, et des moyens de traitement et d'analyse de cette image, décidant de la reconnaissance ou de la non-reconnaissance de l'individu.

En première approche, cette technique est séduisante, car elle semble garantir que l'individu présent est bien celui que le système a identifié, et non un tiers mal intentionné.

Une analyse plus poussée montre cependant que cela n'est pas le cas. Il est en effet relativement aisé, pour un pirate, de contourner le système, par exemple en prélevant le signal délivré par le capteur lors de la reconnaissance d'un individu autorisé, puis de reproduire le même signal pour le fournir aux moyens de traitement et d'analyse. Ces derniers concluront alors à une reconnaissance positive, en l'absence de l'individu autorisé.

Il apparaît donc clairement que les systèmes connus n'apportent pas un niveau de sécurité suffisant, pour de nombreuses applications. Cela est dû notamment au fait que ces systèmes mettent en œuvre des éléments séparés, ce qui implique des flux de données sensibles facilement accessibles et réexploitables entre des éléments séparés.

On a pensé à regrouper dans un même boîtier, ou sur un même circuit imprimé, ces éléments séparés. Mais cela ne change pas le problème, même si cela peut le rendre un peu plus complexe. Les données sensibles circulent sur un bus, par exemple entre le capteur qui relève l'empreinte et le microprocesseur qui la traite et l'analyse. Dès lors, il est possible, pour une personne mal intentionnée, avec des moyens relativement peu complexes, de détecter les signaux circulant sur ce bus, ou de transmettre via ce bus de fausses données au microprocesseur.

Il est à noter que l'identification et l'analyse de ce problème font en eux-mêmes partie de l'invention.

Au-delà de cette forte vulnérabilité des systèmes existants, se pose également le problème important de la protection des informations privées et fortement confidentielles que constituent les informations biométriques. En effet, du fait de l'accessibilité des flux de données codant la caractéristique biométrique, il est possible de créer illicitement une base de données, en vue d'une utilisation interdite par les textes de loi. Il serait par exemple envisageable d'utiliser une telle base de données pour en extraire des caractéristiques individuelles, qui permettraient un ciblage commercial non autorisé par l'individu.

Tant que ces problèmes ne sont pas résolus, il n'est bien sûr ni souhaitable ni envisageable que ces techniques biométriques soient largement utilisées, par exemple dans le cadre d'applications gouvernementales ou bancaires.

L'invention a notamment pour objectif d'apporter une solution à ces problèmes des techniques de l'art antérieur.

Plus précisément, un objectif de l'invention est de fournir une technique permettant l'utilisation de caractéristiques biométriques de façon sûre et fiable.

Notamment, l'invention a pour objectif de fournir une telle technique, qui ne permette pas à un pirate potentiel de recueillir et réutiliser des données biométriques d'un tiers.

Un autre objectif de l'invention est de fournir une telle technique, garantissant la confidentialité des empreintes biométriques d'un individu.

L'invention a également pour objectif de fournir une telle technique, qui

puisse être mise en œuvre industriellement à grande échelle, avec un coût de revient acceptable.

Ces objectifs, ainsi que d'autres qui apparaîtront par la suite, sont atteints selon l'invention à l'aide d'un dispositif de reconnaissance d'au moins un individu, comprenant, dans un circuit intégré monolithique obtenu par l'intégration sur un même substrat de silicium de :

- au moins un capteur d'informations biométriques,
- des moyens de traitement desdites informations biométriques,
- des moyens cryptographiques, délivrant au moins une donnée cryptée représentative d'au moins une partie desdites informations biométriques et/ou d'une information de reconnaissance correspondante, et
- des moyens de protection, empêchant l'accès aux données transitant, stockées et/ou traitées dans ledit circuit intégré monolithique, pour former un périmètre sécurisé,

de façon que les données échangées par le ou lesdits capteurs, lesdits moyens de traitement et lesdits moyens cryptographiques, et notamment lesdites informations biométriques, soient conservées uniquement dans ledit circuit intégré monolithique, restant inaccessibles depuis l'extérieur, et que seules des données cryptées soient délivrées à l'extérieur dudit circuit intégré monolithique.

Ainsi, on empêche l'accès aux informations biométriques, que ce soit pour les réutiliser de façon mal intentionnée ou pour les enregistrer. On garantit donc efficacement la confidentialité et la sécurité, c'est-à-dire l'exactitude de l'identification.

Le fait que tous les moyens soient regroupés dans un module monobloc rend impossible l'accès aux données circulant à l'intérieur. Les moyens cryptographiques permettent de ne laisser sortir que des données non interprétables par un tiers. Selon l'invention, ce module monobloc unique est un circuit intégré monolithique. Cette approche nouvelle et inventive dans ce domaine technique s'avère très efficace, en termes de protection, et aisée à mettre

en œuvre de façon industrielle, tout en permettant de fournir des dispositifs de faible taille et peu consommateurs d'énergie.

Le ou lesdits capteurs sont intégrables sur silicium. Cela permet une fabrication simplifiée (ajout d'une couche supplémentaire correspondant au capteur lors de la fabrication du composant par exemple) et surtout une bonne sécurisation de l'ensemble.

Enfin, ledit circuit intégré monolithique comprend des moyens de protection, ou de sécurisation, empêchant l'accès aux données transitant, stockées et/ou traitées dans ledit circuit intégré monolithique, de façon à définir un périmètre sécurisé. Cela permet de renforcer encore la sécurité, c'est-à-dire de garantir au mieux le non-accès par des tiers aux informations biométriques.

Lesdits moyens de protection empêchant l'accès aux données comprennent au moins un des moyens appartenant notamment au groupe comprenant :

- des moyens de surveillance de l'alimentation électrique dudit circuit intégré monolithique ;
- des moyens de surveillance des caractéristiques d'une horloge synchronisant le fonctionnement dudit dispositif ;
- des moyens de contrôle de la température dudit circuit intégré monolithique;
- des moyens de brouillage des effets électromagnétiques induits par les traitements internes au dispositif ;
- des moyens de protection anti-rayonnement ;
- des moyens de blindage électromagnétiques ;
- des moyens de blindage physique destinés à prévenir et/ou détecter toute tentative d'intrusion physique et/ou électrique sur le dispositif ;
- des moyens de brouillage des informations transitant, traitées et/ou stockées dans le circuit intégré monolithique.

Lesdites informations biométriques traitées par le dispositif de l'invention peuvent être de tout type adéquat. Elles peuvent en particulier appartenir au

groupe comprenant :

- des empreintes digitales ;
- des empreintes vocales ;
- des empreintes oculaires ;
- des caractéristiques morphologiques ;
- des caractéristiques comportementales.

Des combinaisons de ces informations sont bien sûr possibles.

De façon avantageuse, le ou lesdits capteurs peuvent notamment appartenir au groupe comprenant :

- des capteurs thermiques ;
- des capteurs de pression ;
- des capteurs optiques ;
- des capteurs de mouvement ;
- des capteurs de rayonnement ;
- des capteurs de caractéristiques électriques ;
- des capteurs de formes physiques.

Par ailleurs, lesdits moyens de traitement comprennent avantageusement des moyens de mise en forme d'au moins un signal délivré par au moins un desdits capteurs et des moyens d'extraction dudit signal mis en forme d'au moins un caractère pertinent, formant une signature numérique permettant d'identifier de manière unique un individu.

Selon un mode de réalisation avantageux de l'invention, lesdits moyens cryptographiques délivrent une signature cryptographique, calculée à l'aide d'au moins une clé stockée dans une unité de stockage dudit circuit intégré monolithique.

De façon préférentielle, ladite signature cryptographique tient compte également d'au moins un paramètre aléatoire généré et communiqué par des moyens indépendants dudit circuit intégré monolithique.

Il peut par exemple s'agir d'une donnée fournie par un dispositif de contrôle d'accès, d'une donnée horodatée et/ou d'une donnée fournie par

l'utilisateur. Cela permet d'éviter le risque de "rejeu" par un tiers qui aurait pu enregistrer la signature cryptée.

En fonction de cette signature, des moyens extérieurs peuvent mettre en œuvre une reconnaissance de l'individu.

Selon une variante particulière de l'invention, le dispositif peut effectuer lui-même cette opération. Dans ce cas, il comprend des moyens de reconnaissance d'au moins un individu, en fonction de données de référence stockées dans ledit circuit intégré monolithique.

Préférentiellement, lesdits moyens de reconnaissance délivrent une information de reconnaissance, indiquant si un individu est ou non reconnu, ladite information de reconnaissance étant cryptée avant d'être émise à l'extérieur dudit module.

Par ailleurs, le dispositif de l'invention comprend avantageusement, dans ledit circuit intégré monolithique, une unité de stockage comprenant au moins un des éléments appartenant au groupe comprenant :

- au moins une clé cryptographique ;
- au moins un mécanisme de traitement sécurisé de clés cryptographiques ;
- au moins une donnée de référence représentative d'un individu ;
- des données et/ou des programmes nécessaires à la mise en œuvre des moyens présents dans ledit circuit intégré monolithique.

Ladite unité de stockage comprend de façon avantageuse au moins une mémoire de données numériques, appartenant par exemple au groupe comprenant les mémoires flash, les mémoires EEPROM, les mémoires EPROM, les mémoires ROM, les mémoires RAM, les mémoires FeRAM, les mémoires MRAM, les mémoires magnétiques.

Selon un mode particulier de mise en œuvre de l'invention, le circuit intégré monolithique comprend un capteur d'empreintes digitales, délivrant une image d'empreinte, des moyens de traitement de l'image générée et des moyens d'extraction de minuties sur l'image traitée.

Il s'agit d'un mode de mise en œuvre simple et efficace.

De façon préférentielle, lesdits moyens de cryptographie mettent en œuvre au moins un accélérateur de calculs matériel.

L'invention concerne également un procédé de reconnaissance d'au moins un individu, mettant en œuvre un ou plusieurs dispositifs tels que décrits ci-dessus. Un tel procédé comprend notamment les étapes suivantes, mise en œuvre intégralement à l'intérieur d'un circuit intégré monolithique :

- obtention d'informations biométriques dudit individu, à l'aide d'au moins un capteur intégré audit circuit intégré monolithique ;
- traitement desdites informations biométriques ;
- cryptage d'au moins une partie desdites informations biométriques et/ou d'une information de reconnaissance correspondante ;
- transmission vers l'extérieur des données cryptées,

de façon que les données échangées par le ou lesdits capteurs, lesdits moyens de traitement et lesdits moyens cryptographiques, et notamment lesdites informations biométriques, soient conservées uniquement dans ledit circuit intégré monolithique, restant inaccessibles depuis l'extérieur, et que seules des données cryptées soient délivrées à l'extérieur dudit circuit intégré monolithique.

De façon avantageuse, ledit circuit intégré monolithique définit un périmètre sécurisé, en mettant en œuvre des moyens de protection empêchant l'accès aux données transitant, stockées ou traitées dans ledit circuit intégré monolithique.

Préférentiellement, un tel procédé met en œuvre au moins un dispositif de reconnaissance comprenant ledit circuit intégré monolithique et au moins un dispositif de contrôle d'accès communiquant avec ledit dispositif, apte à recevoir et traiter des données cryptées délivrées par le ou lesdits dispositifs de reconnaissance, et à autoriser ou à interdire en conséquence un accès à au moins une donnée, au moins un objet et/ou au moins un lieu.

L'invention concerne encore de tels dispositifs de contrôle d'accès, comprenant des moyens d'autorisation ou d'interdiction d'accès à au moins une

donnée, au moins un objet et/ou au moins un lieu, et des moyens pour recevoir et traiter des données cryptées délivrées par au moins dispositif de reconnaissance d'au moins un individu tel que décrit plus haut.

L'invention concerne également les systèmes de contrôle d'accès à au moins une donnée, au moins un objet et/ou au moins un lieu, mettant en œuvre au moins dispositif de reconnaissance d'au moins un individu et au moins un dispositif de contrôle d'accès tels que décrits ci-dessus.

Enfin, l'invention concerne les applications d'au moins un tel dispositif de reconnaissance d'au moins un individu à au moins un des domaines appartenant au groupe comprenant :

- le contrôle d'accès physique ;
- le contrôle d'accès logique ;
- l'identification du porteur dudit dispositif ;
- la mise en œuvre d'objets nomades ;
- les services bancaires ;
- les signatures électroniques.

Ces caractéristiques et avantages, ainsi que d'autres, apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation préférentiel de l'invention, donnée à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- la figure 1 est un schéma fonctionnel illustrant la structure d'un dispositif de reconnaissance selon l'invention ;
- la figure 2 présente un exemple de système d'accès sécurisé mettant en œuvre l'invention.

L'invention concerne donc une nouvelle approche des systèmes biométriques, reposant notamment sur la mise en œuvre de moyens cryptographiques, permettant un traitement adapté des informations sensibles, relatives à un individu, de façon qu'une empreinte biométrique non cryptée ne soit jamais accessible à un tiers.

Selon l'invention, comme on le verra par la suite, les moyens mis en

œuvre sont regroupés dans une « puce » unique, sur laquelle est notamment intégré le ou les capteurs mis en œuvre. Il n'y a ainsi aucune circulation des informations sensibles (notamment l'empreinte biométrique) en dehors de la puce, et il n'est donc pas possible de les relever ou de les remplacer frauduleusement.

En d'autres termes, l'invention prévoit l'intégration du système biométrique complet dans un circuit intégré monolithique, définissant un environnement parfaitement protégé, correspondant à un périmètre sécurisé au-delà duquel l'empreinte biométrique d'un individu ne sort pas.

Des moyens de protection sont de plus prévus, dans le circuit intégré, pour renforcer la sécurisation, en empêchant l'accès aux données.

La figure 1 présente, de façon fonctionnelle, un mode de réalisation d'un dispositif selon l'invention, détaillant les différents éléments fonctionnels se trouvant sur le circuit intégré monolithique.

Ce dispositif comprend tout d'abord un capteur 11. Il peut s'agir de tout type de composant électronique, sans aucune restriction, dès lors qu'intégrable sur silicium, permettant la conversion d'une information biométrique physique caractéristique d'un individu (par exemple : empreinte digitale, empreinte vocale, empreinte oculaire...), en une information électrique exploitable par une chaîne de traitement numérique.

Ces capteurs peuvent notamment appartenir au groupe comprenant :

- des capteurs thermiques ;
- des capteurs de pression ;
- des capteurs optiques ;
- des capteurs de mouvement ;
- des capteurs de rayonnement ;
- des capteurs de caractéristiques électriques ;
- des capteurs de formes physiques.

Ils permettent par exemple la détection des informations biométriques suivantes :

- empreintes digitales ;

- empreintes vocales ;
- empreintes oculaires ;
- caractéristiques morphologiques ;
- caractéristiques comportementales.

Dans certains cas particuliers, plusieurs capteurs peuvent être associés dans un même dispositif.

Le signal électrique 121 délivré par le capteur alimente des moyens 12 de mise en forme. Il peut notamment s'agir d'un élément analogique ou numérique permettant le traitement de l'information issue du capteur pour l'adapter au dispositif d'extraction de caractères pertinents. Il pourra, par exemple, consister en une unité de traitement d'image autorisant la reconstruction de l'image du caractère biométrique saisie de façon imparfaite par le capteur, pour la rendre conforme à l'image originale.

Le signal mis en forme 121 est ensuite dirigé vers des moyens 13 d'extraction de caractères pertinents. Ces moyens permettent, par traitement numérique suivant des algorithmes dépendant du caractère physique traité, de compresser la grande quantité d'informations saisies par le capteur en extrayant une sorte de signature numérique représentative, de façon unique, de l'individu.

Selon l'invention, cette signature sécurisée ne sort pas du périmètre sécurisé 17 décrit par la suite, c'est-à-dire du circuit intégré monolithique. Elle n'est donc jamais accessible. Seule une version cryptée 141 est délivrée vers l'extérieur.

Pour cela, le dispositif de l'invention comprend, dans le circuit intégré monolithique, des moyens cryptographiques 14, qui calculent une signature cryptographique (cryptage) de l'information numérique représentant les caractères pertinents en utilisant un algorithme cryptographique, tel que par exemple l'un des algorithmes RSA, Courbes Elliptiques, DES, Triple DES, ou AES.

Les clés nécessaires pour effectuer ce traitement sont stockées dans une unité de stockage 15 sécurisée.

La signature cryptographique calculée 141 prend en compte

préférentiellement non seulement l'information numérique représentant les caractères pertinents, mais également au moins un paramètre aléatoire 142 généré et communiqué par le monde extérieur au système, afin d'éviter les possibilités de « rejeu ». Il ne faut pas, en effet, qu'une signature cryptographique qui aurait été enregistrée puisse être réutilisée. Ce paramètre aléatoire peut être une donnée déterminée par un dispositif de contrôle d'accès qui communique avec le dispositif (et qui validera la signature en conséquence), une donnée horodatée, un code fourni par l'individu, ...

La signature calculée 141 est émise vers l'extérieur par le biais d'une sortie 142.

Ainsi, seuls la signature et le(s) paramètre(s) aléatoire(s) circulent à l'extérieur du périmètre sécurisé. Ils permettent la reconnaissance de la signature par un dispositif extérieur de contrôle d'accès adapté.

Selon une variante de réalisation, on prévoit, à l'intérieur du circuit intégré monolithique, des moyens 16 de reconnaissance. Il s'agit de moyens optionnels, qui rendent le dispositif autonome en permettant la reconnaissance de l'individu en recherchant les caractères pertinents issus de la saisie de l'information biométrique dans une base de caractères de référence, représentant par exemple un ensemble d'individus autorisés, stockée dans l'unité de stockage 15 sécurisée.

La sortie 161 permet d'indiquer si l'individu est reconnu. L'information 151 peut (et devrait) être une signature cryptographique de sorte que le résultat de la recherche ne puisse être corrompu ou falsifié.

L'unité de stockage 15, qui peut être une mémoire de tout type (flash, EEPROM, EPROM, ROM, RAM, FeRAM, MRAM, magnétiques), renferme l'ensemble des informations (données et programmes) nécessaires à la gestion du système global. Elle contient, en particulier, les clés nécessaires aux algorithmes cryptographiques intégrés, et l'ensemble des mécanismes nécessaires à la manipulation sécurisée de ces clés (changement, génération...)

Si l'unité de reconnaissance est intégrée au circuit intégré monolithique, cette unité de stockage 15 peut également contenir une base de caractères

pertinents de référence permettant de déterminer si un individu fait partie d'un ensemble d'individus autorisés.

Le dispositif de reconnaissance de l'invention peut également contenir, à l'intérieur ou à l'extérieur du périmètre sécurisé, des moyens spécifiques à une ou plusieurs applications auxquelles il est destiné (stockage de données, dans des applications telles que les téléphones portables, d'informations personnelles, pour les applications telles que les "cartes de citoyen" ou les cartes relatives à la santé, gestion de comptes, pour des applications de type porte-monnaie électronique, gestion de communication, avec un dispositif distant, tel qu'un serveur ou une machine, ...).

Avantageusement, l'ensemble des moyens détaillés ci-dessus sont placés à l'intérieur d'un périmètre sécurité 17, c'est-à-dire du circuit intégré monolithique. Il convient de noter qu'il s'agit d'un périmètre physique dans lequel un certain nombre de moyens sont installés pour interdire l'accès aux informations qui transitent, sont stockées ou traitées par tout moyen d'attaque connu.

Les moyens de sécurisation, ou de protection, peuvent notamment comprendre :

- des moyens de surveillance de l'alimentation électrique dudit dispositif ;
- des moyens de surveillance des caractéristiques de l'horloge synchronisant le fonctionnement dudit dispositif ;
- des moyens de contrôle de la température dudit dispositif ;
- des moyens de brouillage des effets électromagnétiques induits par les traitements internes au dispositif ;
- des moyens de protection anti-rayonnement ;
- des moyens de blindage électromagnétiques ;
- des moyens de blindage physique destinés à prévenir et/ou détecter toute tentative d'intrusion physique ou électrique sur le dispositif ;
- des moyens de brouillage des informations transitant, traitées, ou stockées dans le dispositif.

A titre d'exemple particulier, on considère ci-après le cas de la reconnaissance d'une empreinte digitale. Dans ce cas :

- le capteur 11 peut être un capteur thermique ;
- les moyens 12 de mise en forme effectuent un traitement numérique de l'image correspondante ;
- les moyens 13 d'extraction de caractères pertinents comprennent un calculateur réalisant l'extraction des minuties d'une empreinte digitale.

Comme déjà mentionné, le dispositif de l'invention est réalisé sous la forme d'un circuit intégré. L'implémentation du dispositif consiste alors en l'assemblage sur un même composant d'un capteur d'empreintes digitales, d'un circuit de traitement de l'image générée, d'un circuit d'extraction de paramètres pertinents (IP) basé par exemple sur le principe d'extraction de minuties, et d'un microcontrôleur sécurisé permettant la gestion de l'ensemble, ainsi que le calcul cryptographique (par le biais d'accélérateurs matériels adaptés).

La reconnaissance de l'empreinte peut être gérée à l'extérieur du composant ou à l'aide d'un logiciel adapté. L'unité de stockage 15 sera composée par exemple d'un espace de mémoire flash intégrée dans le composant.

Autour de ces blocs de base, un ensemble de moyens permettra de garantir la résistance de l'ensemble à toutes les attaques connues à ce jour.

La résistance de l'ensemble est ainsi évaluable, et évaluée, suivant les critères communs, avec une cible de protection élevée (EAL 4+) correspondant à ce qui se fait de mieux en matière de sécurité à ce jour. Il est à noter que ce type d'évaluation ne pourrait en aucun cas être obtenu ni approché avec les méthodes classiques disponibles selon l'art antérieur.

Il s'agit donc bien d'un ensemble monolithique, fabriqué classiquement par exemple par couches successives, selon des techniques de fabrication de circuits intégrés connus en soi. En ce qui concerne l'intégration du capteur, la mise en œuvre d'une telle approche est également connue, notamment pour des capteurs photosensibles, par exemple en technologie CMOS, dans le domaine des

caméras et des appareils photographiques numériques. On pourra notamment se référer aux nombreux documents de brevet relatifs à ces sujets listés dans la classe H01L27/14 de la CIB, et par exemple au document de brevet FR-2819101, dont le titulaire est ATMEL, et ayant pour titre « capteur photosensible en technologie des circuits intégrés » (non publiée à la date de priorité de la présente demande), ou encore

Les applications de ce type de composant sont toutes les applications où il est nécessaire de conditionner un accès physique ou logique (données, local...) à la présentation d'un « code » connu par la personne autorisée. En l'espèce, le « code » est une information biométrique cryptée.

Le domaine d'application de l'invention est donc très vaste. Il va du contrôle d'accès à une carte à puce (auquel cas l'algorithme de reconnaissance est placé sur la carte), au contrôle d'accès à une chambre d'hôtel, en passant par le contrôle d'accès à un produit nomade (PDA, téléphone mobile...).

Plus généralement, l'invention trouve des applications dans tous les domaines suivants :

- le contrôle d'accès physique ;
- le contrôle d'accès logique ;
- l'identification du porteur dudit dispositif ;
- la mise en œuvre d'objets nomades ;
- les services bancaires :
- les signatures électroniques.

La figure 2 illustre un exemple de système mettant en œuvre des dispositifs de reconnaissance tels que décrits plus haut.

Il comprend une pluralité de dispositifs 21 de reconnaissance, distribués à un ensemble d'individus, et au moins un dispositif de contrôle d'accès 22, capable de recevoir et de traiter les informations cryptées 23 produites par un dispositif 21, afin par exemple de commander l'ouverture d'une porte ou l'accès à un fichier.

Le dispositif de contrôle d'accès 22 comprend donc des moyens pour fournir une donnée aléatoire 142 pour le cryptage, et pour effectuer le décryptage

correspondant.

Les échanges de données entre le dispositif 21 de reconnaissance et le dispositif 22 de contrôle d'accès peuvent se faire selon toutes les techniques adéquates (contact à l'aide d'un lecteur adapté, transmission à distance par voie hertzienne ou infrarouge, etc.).

Selon les applications, on peut prévoir un unique dispositif de contrôle d'accès 22 (accès à un local) ou un nombre élevé de tels dispositifs de réception (cas des applications bancaires par exemple).

Le dispositif 21 de reconnaissance peut former, ou être monté dans, un objet portatif (correspondant par exemple à une clé ou aux cartes bancaires actuelles), ou être intégré à un objet (ordinateur, portière de véhicule, ...) ou à une pièce, un bâtiment ou un site.

REVENDICATIONS

1. Dispositif de reconnaissance d'au moins un individu, caractérisé en ce qu'il comprend, dans un circuit intégré monolithique obtenu par l'intégration sur un même substrat de silicium de :

- au moins un capteur d'informations biométriques,
- des moyens de traitement desdites informations biométriques,
- des moyens cryptographiques, délivrant au moins une donnée cryptée représentative d'au moins une partie desdites informations biométriques et/ou d'une information de reconnaissance correspondante, et
- des moyens de protection, empêchant l'accès aux données transitant, stockées et/ou traitées dans ledit circuit intégré monolithique, pour former un périmètre sécurisé,

de façon que les données échangées par le ou lesdits capteurs, lesdits moyens de traitement et lesdits moyens cryptographiques, et notamment lesdites informations biométriques, soient conservées uniquement dans ledit circuit intégré monolithique, restant inaccessibles depuis l'extérieur, et que seules des données cryptées soient délivrées à l'extérieur dudit circuit intégré monolithique.

2. Dispositif de reconnaissance d'au moins un individu selon la revendication 1, caractérisé en ce que lesdits moyens de protection empêchant l'accès aux données comprennent au moins un des moyens appartenant au groupe comprenant :

- des moyens de surveillance de l'alimentation électrique dudit circuit intégré monolithique;
- des moyens de surveillance des caractéristiques d'une horloge synchronisant le fonctionnement dudit dispositif ;
- des moyens de contrôle de la température dudit circuit intégré monolithique;
- des moyens de brouillage des effets électromagnétiques induits par les traitements internes au dispositif ;

- des moyens de protection anti-rayonnement ;
- des moyens de blindage électromagnétiques ;
- des moyens de blindage physique destinés à prévenir et/ou détecter toute tentative d'intrusion physique et/ou électrique sur le dispositif ;
- des moyens de brouillage des informations transitant, traitées et/ou stockées dans le dispositif.

3. Dispositif de reconnaissance d'au moins un individu selon l'une quelconque des revendications 1 et 2, caractérisé en ce que lesdites informations biométriques appartiennent au groupe comprenant :

- des empreintes digitales ;
- des empreintes vocales ;
- des empreintes oculaires ;
- des caractéristiques morphologiques ;
- des caractéristiques comportementales.

4. Dispositif de reconnaissance d'au moins un individu selon l'une quelconque des revendications 1 à 3, caractérisé en ce que le ou lesdits capteurs appartiennent au groupe comprenant :

- des capteurs thermiques ;
- des capteurs de pression ;
- des capteurs optiques ;
- des capteurs de mouvement ;
- des capteurs de rayonnement ;
- des capteurs de caractéristiques électriques ;
- des capteurs de formes physiques.

5. Dispositif de reconnaissance d'au moins un individu selon l'une quelconque des revendications 1 à 4, caractérisé en ce que lesdits moyens de traitement comprennent des moyens de mise en forme d'au moins un signal délivré par au moins un desdits capteurs et des moyens d'extraction dudit signal mis en forme d'au moins un caractère pertinent, formant une signature numérique

permettant d'identifier de manière unique un individu.

6. Dispositif de reconnaissance d'au moins un individu selon l'une quelconque des revendications 1 à 5, caractérisé en ce que lesdits moyens cryptographiques délivrent une signature cryptographique, calculée à l'aide d'au moins une clé stockée dans une unité de stockage dudit circuit intégré monolithique.

7. Dispositif de reconnaissance d'au moins un individu selon la revendication 8, caractérisé en ce que ladite signature cryptographique tient compte également d'au moins un paramètre aléatoire généré et communiqué par des moyens indépendants dudit circuit intégré monolithique.

8. Dispositif de reconnaissance d'au moins un individu selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il comprend des moyens de reconnaissance d'au moins un individu, en fonction de données de référence stockées dans ledit circuit intégré monolithique.

9. Dispositif de reconnaissance d'au moins un individu selon la revendication 8, caractérisé en ce que lesdits moyens de reconnaissance délivrent une information de reconnaissance, indiquant si un individu est ou non reconnu, ladite information de reconnaissance étant cryptée avant d'être émise à l'extérieur dudit circuit intégré monolithique.

10. Dispositif de reconnaissance d'au moins un individu selon l'une quelconque des revendications 1 à 9, caractérisé en ce que ledit circuit intégré monolithique comprend une unité de stockage comprenant au moins un des éléments appartenant au groupe comprenant :

- au moins une clé cryptographique ;
- au moins un mécanisme de traitement sécurisé de clés cryptographiques ;
- au moins une donnée de référence représentative d'un individu ;
- des données et/ou des programmes nécessaires à la mise en œuvre des moyens présents dans ledit circuit intégré monolithique.

11. Dispositif de reconnaissance d'au moins un individu selon la revendication

10, caractérisé en ce que ladite unité de stockage comprend au moins une mémoire de données numériques.

12. Dispositif de reconnaissance d'au moins un individu selon la revendication 11, caractérisé en ce que ladite ou lesdites mémoires de données numériques appartiennent au groupe comprenant les mémoires flash, les mémoires EEPROM, les mémoires EPROM, les mémoires ROM, les mémoires RAM, les mémoires FeRAM, les mémoires MRAM, les mémoires magnétiques.

13. Dispositif de reconnaissance d'au moins un individu selon l'une quelconque des revendications 1 à 12, caractérisé en ce que ledit circuit intégré monolithique comprend un capteur d'empreintes digitales, délivrant une image d'empreinte, des moyens de traitement de l'image générée et des moyens d'extraction de minuties sur l'image traitée.

14. Dispositif de reconnaissance d'au moins un individu selon l'une quelconque des revendications 1 à 13, caractérisé en ce que lesdits moyens de cryptographie mettent en œuvre au moins un accélérateur de calculs matériel.

15. Procédé de reconnaissance d'au moins un individu, caractérisé en ce qu'il comprend les étapes suivantes, mise en œuvre intégralement à l'intérieur d'un circuit intégré monolithique :

- obtention d'informations biométriques dudit individu, à l'aide d'au moins un capteur intégré audit circuit intégré monolithique ;
- traitement desdites informations biométriques ;
- cryptage d'au moins une partie desdites informations biométriques et/ou d'une information de reconnaissance correspondante ;
- transmission vers l'extérieur des données cryptées,

de façon que les données échangées par le ou lesdits capteurs, lesdits moyens de traitement et lesdits moyens cryptographiques, et notamment lesdites informations biométriques, soient conservées uniquement dans ledit circuit intégré monolithique, restant inaccessibles depuis l'extérieur, et que seules des données cryptées soient délivrées à l'extérieur dudit circuit intégré monolithique.

16. Procédé de reconnaissance d'au moins un individu selon la revendication

15, caractérisé en ce que ledit circuit intégré monolithique définit un périmètre sécurisé, en mettant en œuvre des moyens de protection empêchant l'accès aux données transitant, stockées ou traitées dans ledit circuit intégré monolithique.

17. Procédé de reconnaissance d'au moins un individu selon l'une quelconque des revendications 15 et 16, caractérisé en ce qu'il met en œuvre au moins un dispositif de reconnaissance comprenant ledit circuit intégré monolithique et au moins un dispositif de contrôle d'accès communiquant avec ledit dispositif de reconnaissance, apte à recevoir et traiter des données cryptées délivrées par le ou lesdits dispositifs de reconnaissance, et à autoriser ou à interdire en conséquence un accès à au moins une donnée, au moins un objet et/ou au moins un lieu.

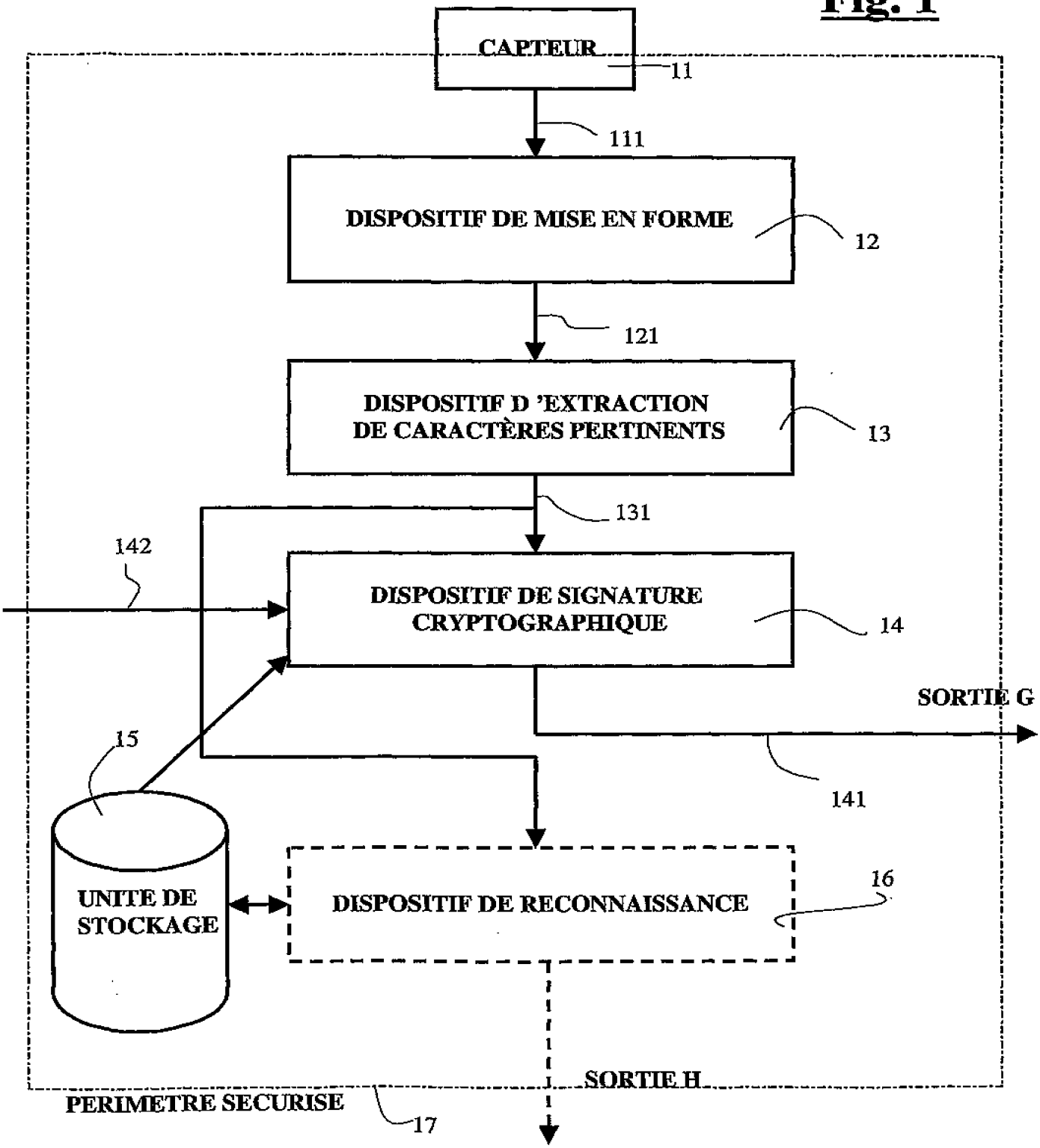
18. Dispositif de contrôle d'accès comprenant des moyens d'autorisation ou d'interdiction d'accès à au moins une donnée, au moins un objet et/ou au moins un lieu, caractérisé en ce qu'il comprend des moyens pour recevoir et traiter des données cryptées délivrées par au moins dispositif de reconnaissance d'au moins un individu selon l'une quelconque des revendications 1 à 14.

19. Système de contrôle d'accès à au moins une donnée, au moins un objet et/ou au moins un lieu, caractérisé en ce qu'il comprend au moins dispositif de reconnaissance d'au moins un individu selon l'une quelconque des revendications 1 à 14 et au moins un dispositif de contrôle d'accès selon la revendication 18.

20. Application d'un dispositif de reconnaissance d'au moins un individu selon l'une quelconque des revendications 1 à 14 et/ou d'un procédé de reconnaissance d'au moins un individu selon l'une quelconque des revendications 15 à 17 à au moins un des domaines appartenant au groupe comprenant :

- le contrôle d'accès physique ;
- le contrôle d'accès logique ;
- l'identification du porteur dudit dispositif ;
- la mise en œuvre d'objets nomades ;
- les services bancaires ;
- les signatures électroniques.

Fig. 1


CAPTEUR
11
111
DISPOSITIF DE MISE EN FORME
12
121
DISPOSITIF D 'EXTRACTION
DE CARACTÈRES PERTINENTS
13
131
142
DISPOSITIF DE SIGNATURE
CRYPTOGRAPHIQUE
14
SORTIE G
15
141
UNITE DE
STOCKAGE
DISPOSITIF DE RECONNAISSANCE
16
SORTIE H
PERIMETRE SECURISE
17

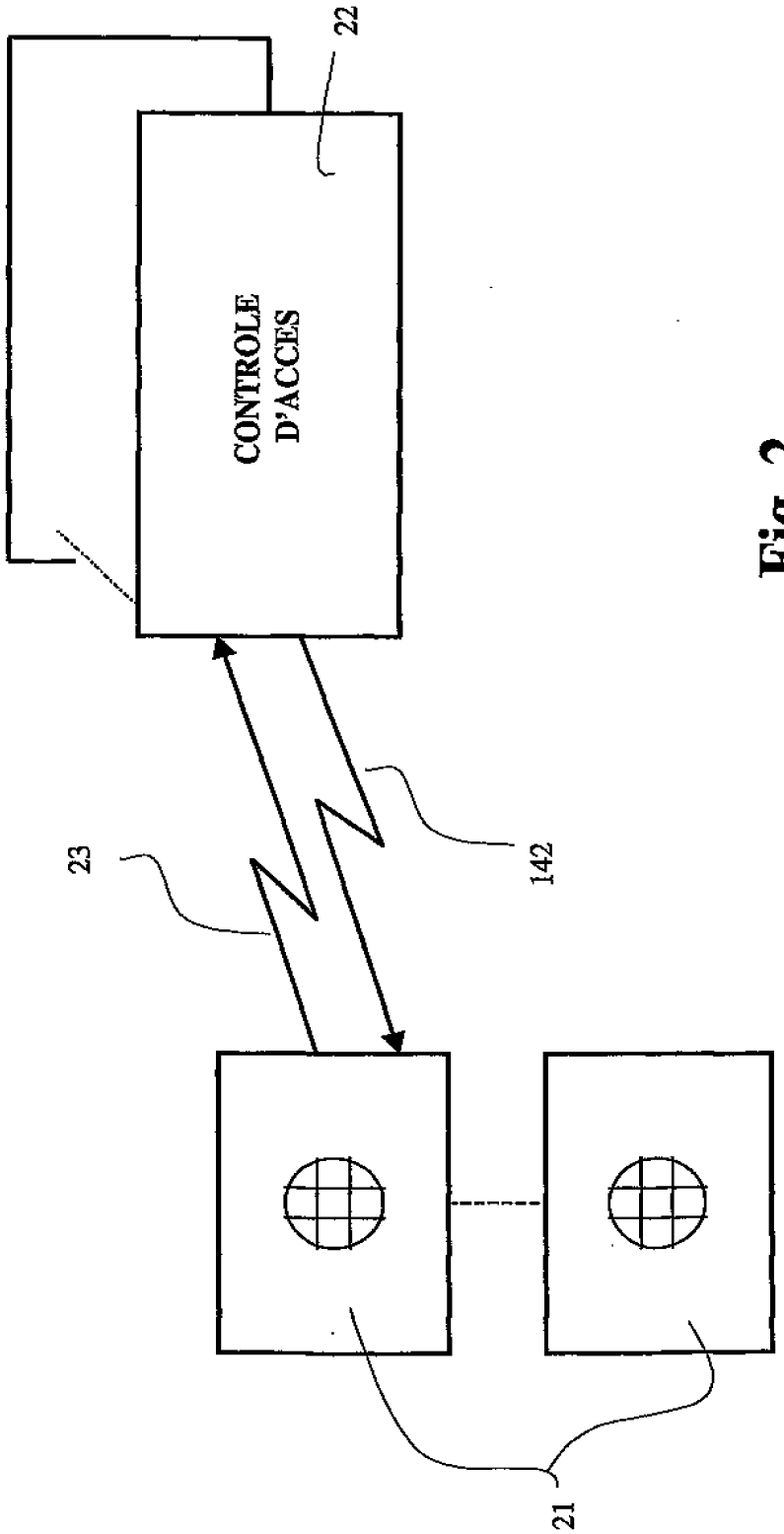


Fig. 2

INTERNATIONAL SEARCH REPORT

Internat Application No
PCT/IB 02/02874

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07C G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO 02 01328 A (BRIZEK JOHN ;HASBUN ROBERT (US); INTEL CORP (US); VOGT JAMES (US)) 3 January 2002 (2002-01-03) page 4, line 14 -page 19, line 4 figures	1-5,8, 10-16, 18-20
Y	WO 00 65770 A (ROWLEY THOMAS E III ;VERIDICOM INC (US)) 2 November 2000 (2000-11-02) abstract page 11, line 18 -page 19, line 10 figures	1-20
Y	EP 1 113 405 A (ST MICROELECTRONICS INC) 4 July 2001 (2001-07-04) paragraph '0036! - paragraph '0041! figures 4-9	1-20

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 January 2003	24/01/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Miltgen, E

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna l Application No
PCT/FR 02/02874

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 070 796 A (SIRBU CORNEL) 6 June 2000 (2000-06-06) abstract column 2, line 28 -column 3, line 37 column 7, line 60 -column 8, line 52 figure 7	1,3-5, 8-12, 15-20
A	WO 98 11750 A (SUBBIAH SUBRAMANIAN ;LI YANG (US); RAO D RAMESK K (US)) 19 March 1998 (1998-03-19) abstract; claims; figures	1,3-7, 10-13, 15-20
A	US 5 864 296 A (UPTON ERIC L) 26 January 1999 (1999-01-26) abstract; claims; figures	1,8,15, 18-20
A	FR 2 774 793 A (BULL CP8) 13 August 1999 (1999-08-13) page 2, line 11 - line 19 page 6, line 27 -page 7, line 7	1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

.nation on patent family members

Inter I Application No
PCT/FR 02/02874

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0201328 A	03-01-2002	AU 7543501 A	08-01-2002
		WO 0201328 A2	03-01-2002
WO 0065770 A	02-11-2000	AU 4250100 A	10-11-2000
		EP 1175749 A1	30-01-2002
		WO 0065770 A1	02-11-2000
EP 1113405 A	04-07-2001	EP 1113405 A2	04-07-2001
		JP 2001249002 A	14-09-2001
US 6070796 A	06-06-2000	FR 2738070 A1	28-02-1997
		FR 2740885 A1	09-05-1997
		AT 217103 T	15-05-2002
		AU 720839 B2	15-06-2000
		AU 6824096 A	12-03-1997
		BG 63764 B1	29-11-2002
		BG 102336 A	30-12-1998
		BR 9610236 A	15-06-1999
		CN 1194043 A	23-09-1998
		CZ 9800408 A3	16-12-1998
		DE 69621042 D1	06-06-2002
		DK 870222 T3	26-08-2002
		EA 1415 B1	26-02-2001
		EP 0870222 A2	14-10-1998
		ES 2176481 T3	01-12-2002
		WO 9707448 A2	27-02-1997
		HU 9900499 A2	28-06-1999
		JP 11511278 T	28-09-1999
		NO 980728 A	20-04-1998
		NZ 503211 A	21-12-2001
		PL 325164 A1	06-07-1998
		PT 870222 T	31-10-2002
		SK 22098 A3	07-10-1998
		TR 9800267 T2	21-07-1998
		ZA 9607077 A	21-05-1997
WO 9811750 A	19-03-1998	US 6219793 B1	17-04-2001
		AU 4341797 A	02-04-1998
		EP 0931430 A2	28-07-1999
		WO 9811750 A2	19-03-1998
US 5864296 A	26-01-1999	JP 3249468 B2	21-01-2002
		JP 10323339 A	08-12-1998
FR 2774793 A	13-08-1999	FR 2774793 A1	13-08-1999
		EP 0985197 A1	15-03-2000
		WO 9941709 A1	19-08-1999
		JP 2000513858 T	17-10-2000

RAPPORT DE RECHERCHE INTERNATIONALE

Demar ternationale No
PCT/FR 02/02874

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07C9/00 G06F1/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07C G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
P,X	WO 02 01328 A (BRIZEK JOHN ;HASBUN ROBERT (US); INTEL CORP (US); VOGT JAMES (US)) 3 janvier 2002 (2002-01-03) page 4, ligne 14 -page 19, ligne 4 figures	1-5,8, 10-16, 18-20
Y	WO 00 65770 A (ROWLEY THOMAS E III ;VERIDICOM INC (US)) 2 novembre 2000 (2000-11-02) abrégé page 11, ligne 18 -page 19, ligne 10 figures	1-20
Y	EP 1 113 405 A (ST MICROELECTRONICS INC) 4 juillet 2001 (2001-07-04) alinéa '0036! - alinéa '0041! figures 4-9	1-20

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
17 janvier 2003	24/01/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Miltgen, E

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	US 6 070 796 A (SIRBU CORNEL) 6 juin 2000 (2000-06-06) abrégé colonne 2, ligne 28 -colonne 3, ligne 37 colonne 7, ligne 60 -colonne 8, ligne 52 figure 7	1,3-5, 8-12, 15-20
A	WO 98 11750 A (SUBBIAH SUBRAMANIAN ;LI YANG (US); RAO D RAMESK K (US)) 19 mars 1998 (1998-03-19) abrégé; revendications; figures	1,3-7, 10-13, 15-20
A	US 5 864 296 A (UPTON ERIC L) 26 janvier 1999 (1999-01-26) abrégé; revendications; figures	1,8,15, 18-20
A	FR 2 774 793 A (BULL CP8) 13 août 1999 (1999-08-13) page 2, ligne 11 - ligne 19 page 6, ligne 27 -page 7, ligne 7	1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs bres de familles de brevets

Dem ternationale No
PCT/FR 02/02874

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0201328	A	03-01-2002	AU	7543501 A	08-01-2002
			WO	0201328 A2	03-01-2002
WO 0065770	A	02-11-2000	AU	4250100 A	10-11-2000
			EP	1175749 A1	30-01-2002
			WO	0065770 A1	02-11-2000
EP 1113405	A	04-07-2001	EP	1113405 A2	04-07-2001
			JP	2001249002 A	14-09-2001
US 6070796	A	06-06-2000	FR	2738070 A1	28-02-1997
			FR	2740885 A1	09-05-1997
			AT	217103 T	15-05-2002
			AU	720839 B2	15-06-2000
			AU	6824096 A	12-03-1997
			BG	63764 B1	29-11-2002
			BG	102336 A	30-12-1998
			BR	9610236 A	15-06-1999
			CN	1194043 A	23-09-1998
			CZ	9800408 A3	16-12-1998
			DE	69621042 D1	06-06-2002
			DK	870222 T3	26-08-2002
			EA	1415 B1	26-02-2001
			EP	0870222 A2	14-10-1998
			ES	2176481 T3	01-12-2002
			WO	9707448 A2	27-02-1997
			HU	9900499 A2	28-06-1999
			JP	11511278 T	28-09-1999
			NO	980728 A	20-04-1998
			NZ	503211 A	21-12-2001
			PL	325164 A1	06-07-1998
			PT	870222 T	31-10-2002
			SK	22098 A3	07-10-1998
			TR	9800267 T2	21-07-1998
			ZA	9607077 A	21-05-1997
WO 9811750	A	19-03-1998	US	6219793 B1	17-04-2001
			AU	4341797 A	02-04-1998
			EP	0931430 A2	28-07-1999
			WO	9811750 A2	19-03-1998
US 5864296	A	26-01-1999	JP	3249468 B2	21-01-2002
			JP	10323339 A	08-12-1998
FR 2774793	A	13-08-1999	FR	2774793 A1	13-08-1999
			EP	0985197 A1	15-03-2000
			WO	9941709 A1	19-08-1999
			JP	2000513858 T	17-10-2000